FIG.1

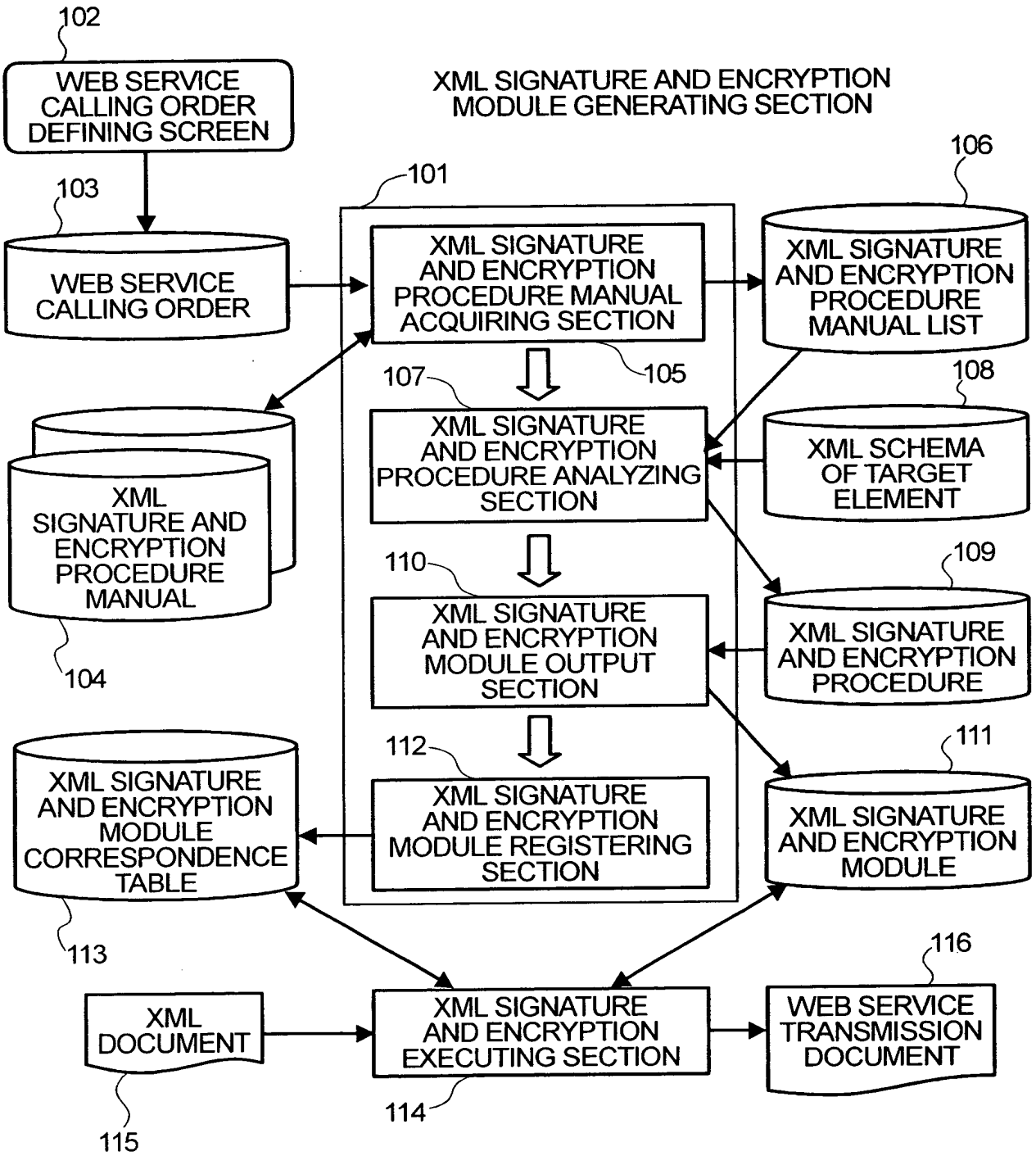

102
WEB SERVICE CALLING ORDER DEFINING SCREEN
XML SIGNATURE AND ENCRYPTION MODULE GENERATING SECTION
106
101
103
WEB SERVICE CALLING ORDER
XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL ACQUIRING SECTION
XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL LIST
105
107
108
XML SIGNATURE AND ENCRYPTION PROCEDURE ANALYZING SECTION
XML SCHEMA OF TARGET ELEMENT
XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL
110
109
XML SIGNATURE AND ENCRYPTION MODULE OUTPUT SECTION
XML SIGNATURE AND ENCRYPTION PROCEDURE
104
112
111
XML SIGNATURE AND ENCRYPTION MODULE CORRESPONDENCE TABLE
XML SIGNATURE AND ENCRYPTION MODULE REGISTERING SECTION
XML SIGNATURE AND ENCRYPTION MODULE
113
116
XML DOCUMENT
XML SIGNATURE AND ENCRYPTION EXECUTING SECTION
WEB SERVICE TRANSMISSION DOCUMENT
115
114

FIG.2

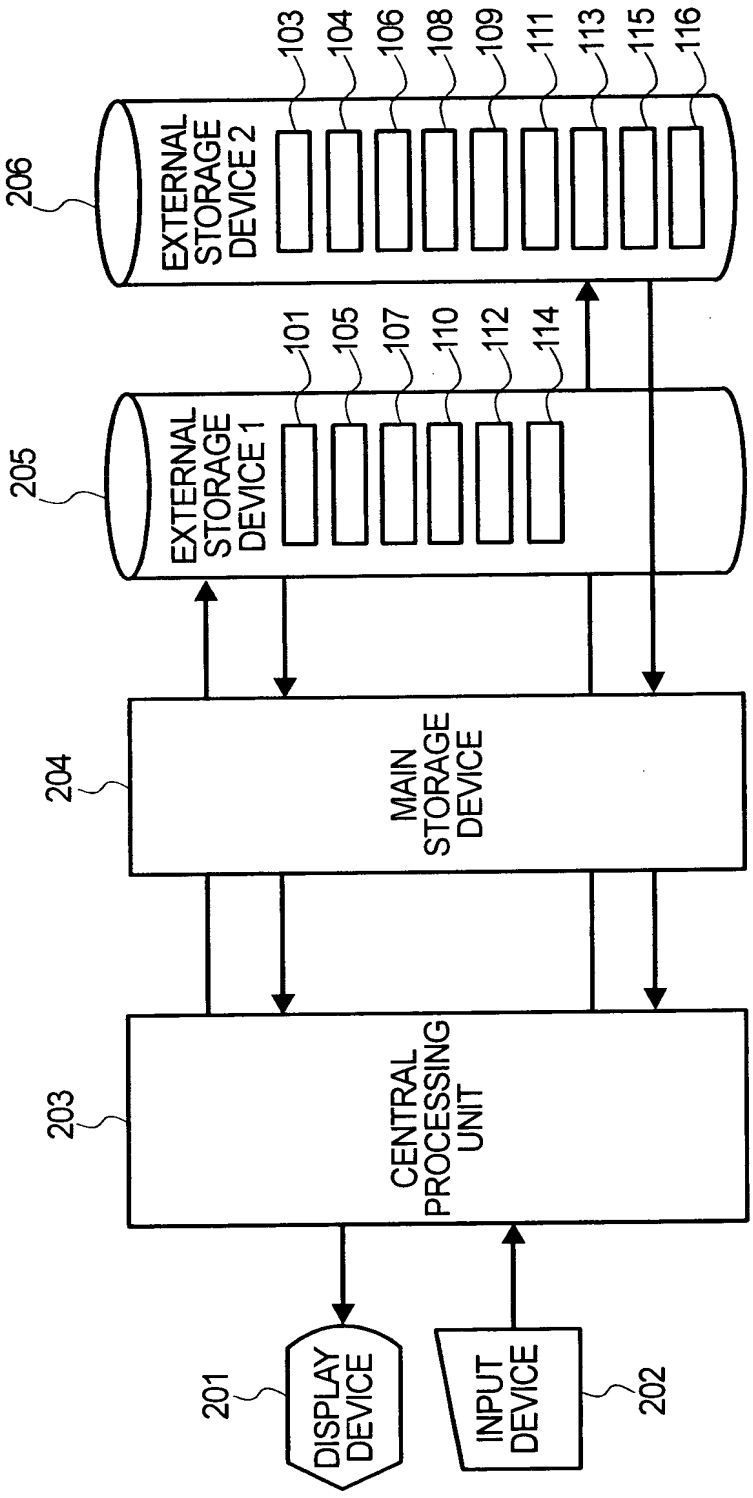

206
EXTERNAL STORAGE DEVICE 2
103
104
106
108
109
111
113
115
116
205
EXTERNAL STORAGE DEVICE 1
101
105
107
110
112
114
204
MAIN STORAGE DEVICE
203
CENTRAL PROCESSING UNIT
201
DISPLAY DEVICE
INPUT DEVICE
202

FIG.3

WEB SERVICE CALLING ORDER DEFINING SCREEN 102

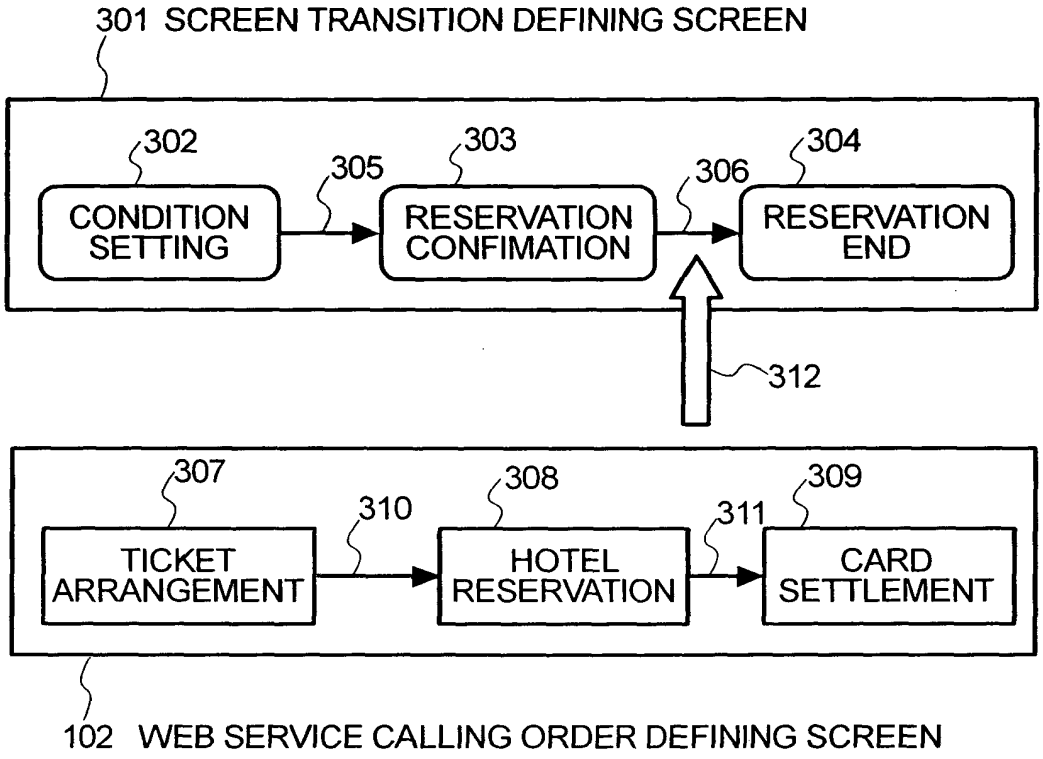


FIG.4

WEB SERVICE CALLING ORDER 103

	401 ID	402 NEXT ID	403 NAME	404 WEB SERVICE URI	405 XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL URI
406	A	B	TICKET ARRANGEMENT	http://www.tickets.com/	http://www.tickets.com/sec
407	B	C	HOTEL RESERVATION	http://www.hotels.com/	http://www.hotels.com/sec
408	C	NONE	CARD SETTLEMENT	http://www.cards.com/	http://www.cards.com/sec

FIG.5

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 104

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 501 CORRESPONDING TO 406

	504 ORDER	505 TARGET ELEMENT	506 OPERATION	507 ALGORITHM
508	1	tickets	ENCRYPTION	AES
509	2	userinfo	ENCRYPTION	DESede
510	3	root	SIGNATURE	DSS

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 502 CORRESPONDING TO 407

	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
511	1	hotels	ENCRYPTION	DESede
512	2	userinfo	ENCRYPTION	AES
513	3	root	SIGNATURE	RSA

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL 503 CORRESPONDING TO 408

	ORDER	TARGET ELEMENT	OPERATION	ALGORITHM
514	1	cardinfo	ENCRYPTION	RSA
515	2	userinfo	SIGNATURE	DSS

FIG.6

XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL ACQUIRING SECTION 105

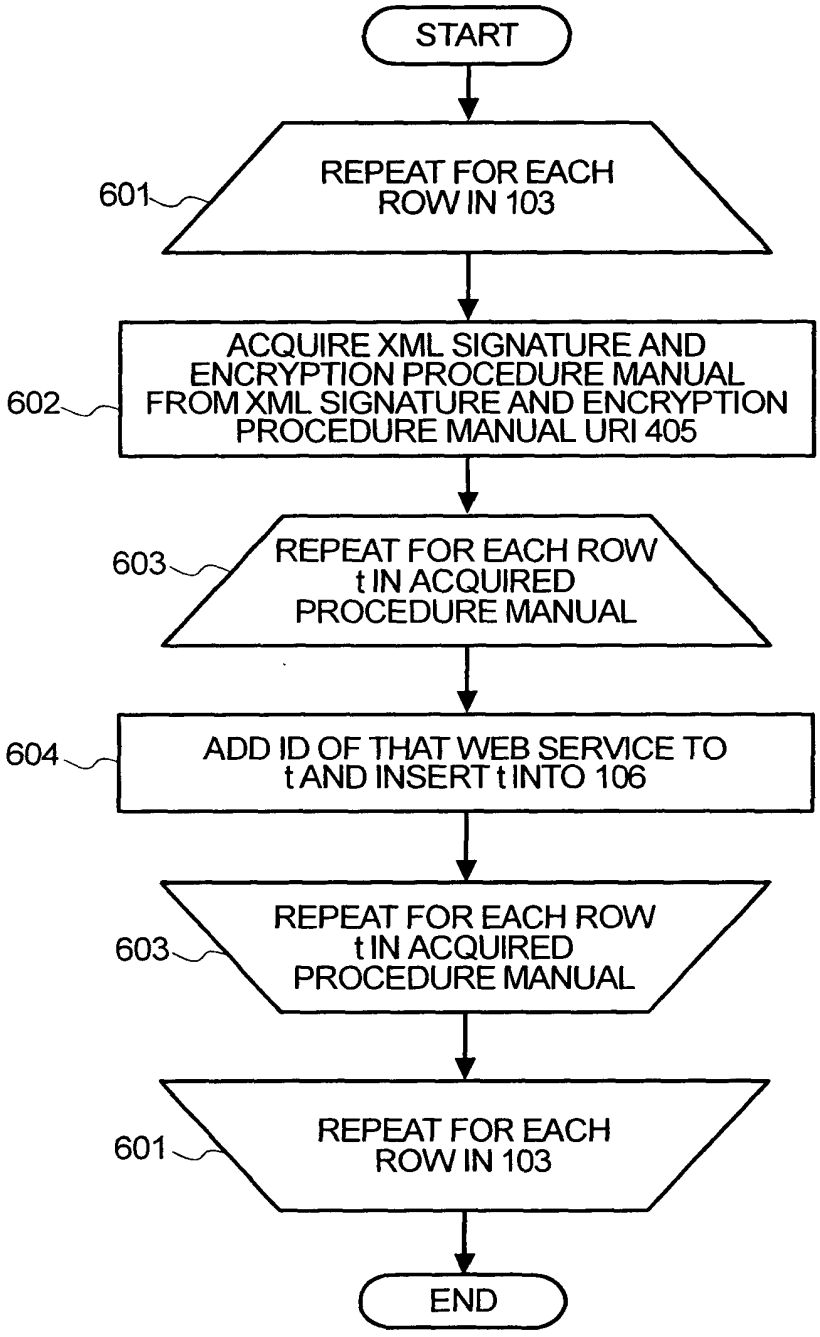


FIG.7

XML SIGNATURE AND
ENCRYPTION PROCEDURE MANUAL LIST 106

	701 ID	702 ORDER	703 TARGET ELEMENT	704 OPERATION	705 ALGORITHM
706	A	1	tickets	ENCRYPTION	AES
707	A	2	userinfo	ENCRYPTION	DESede
708	A	3	root	SIGNATURE	DSS
709	B	1	hotels	ENCRYPTION	DESede
710	B	2	userinfo	ENCRYPTION	AES
711	B	3	root	SIGNATURE	RSA
712	C	1	cardinfo	ENCRYPTION	RSA
713	C	2	userinfo	SIGNATURE	DSS

FIG.8

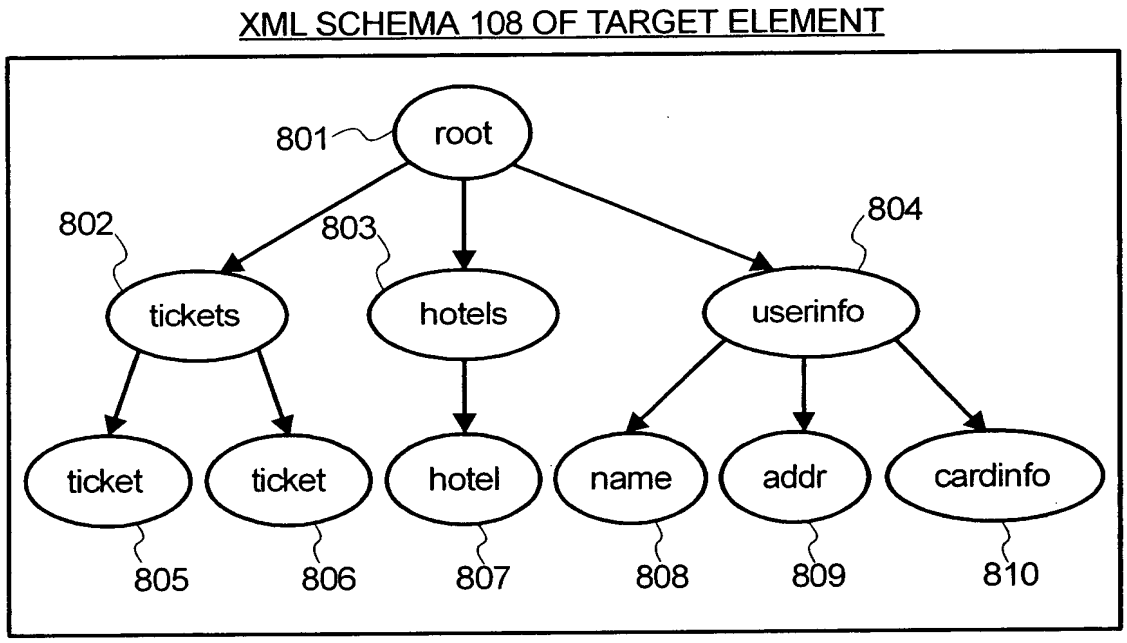

XML SCHEMA 108 OF TARGET ELEMENT
801
root
802
803
804
tickets
hotels
userinfo
ticket
ticket
hotel
name
addr
cardinfo
805
806
807
808
809
810

FIG.9

XML SIGNATURE AND ENCRYPTION PROCEDURE ANALYZING SECTION 107

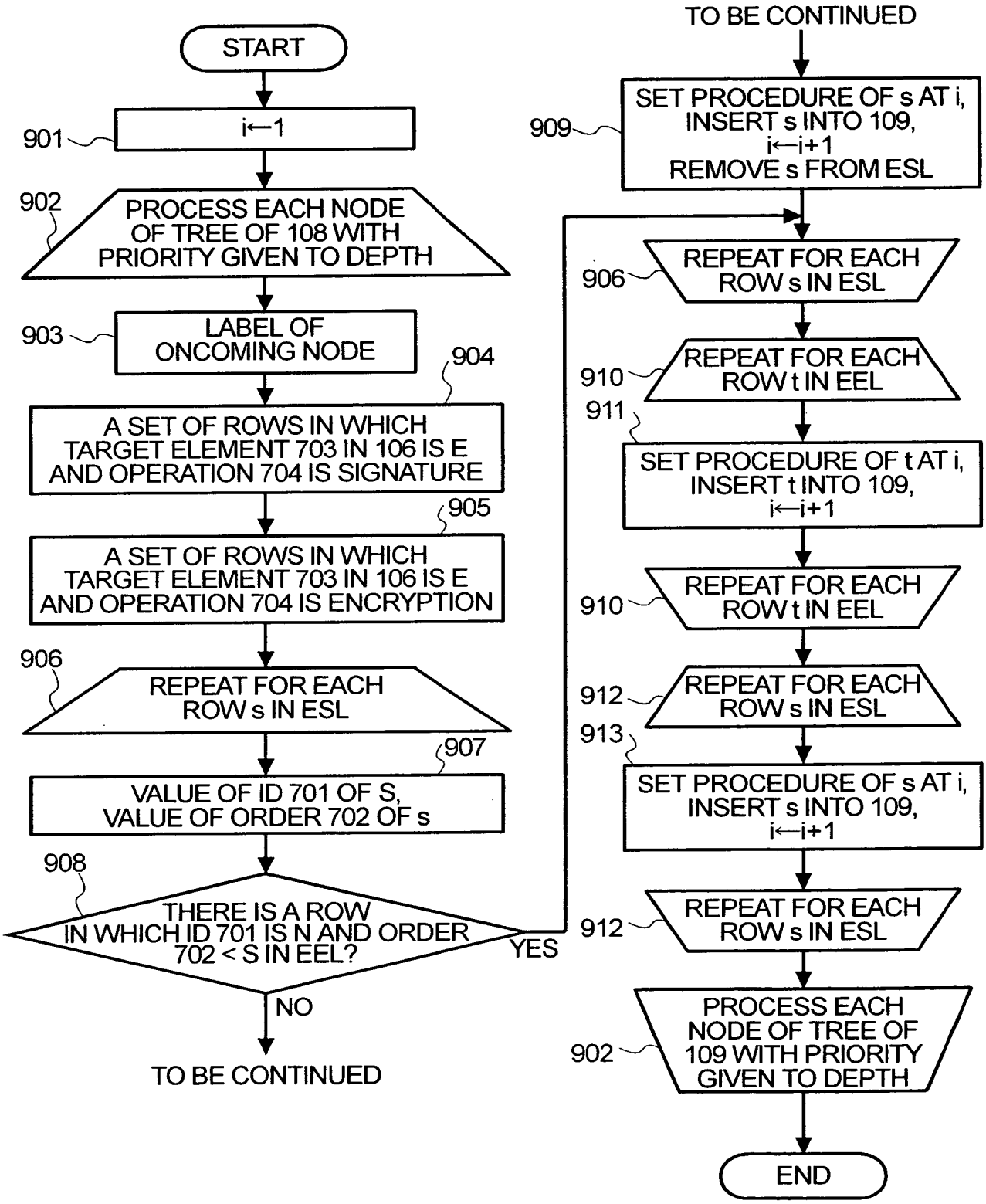


FIG.10

XML SIGNATURE AND ENCRYPTION PROCEDURE 109

	1001 PROCEDURE	1002 ID	1003 ORDER	1004 TARGET ELEMENT	1005 OPERATION	1006 ALGORITHM
1007	1	A	1	tickets	ENCRYPTION	AES
1008	2	B	1	hotels	ENCRYPTION	DESede
1009	3	C	1	cardinfo	ENCRYPTION	RSA
1010	4	C	2	userinfo	SIGNATURE	DSS
1011	5	A	2	userinfo	ENCRYPTION	DESede
1012	6	B	2	userinfo	ENCRYPTION	AES
1013	7	A	3	root	SIGNATURE	DSS
1014	8	B	3	root	SIGNATURE	RSA

FIG.11

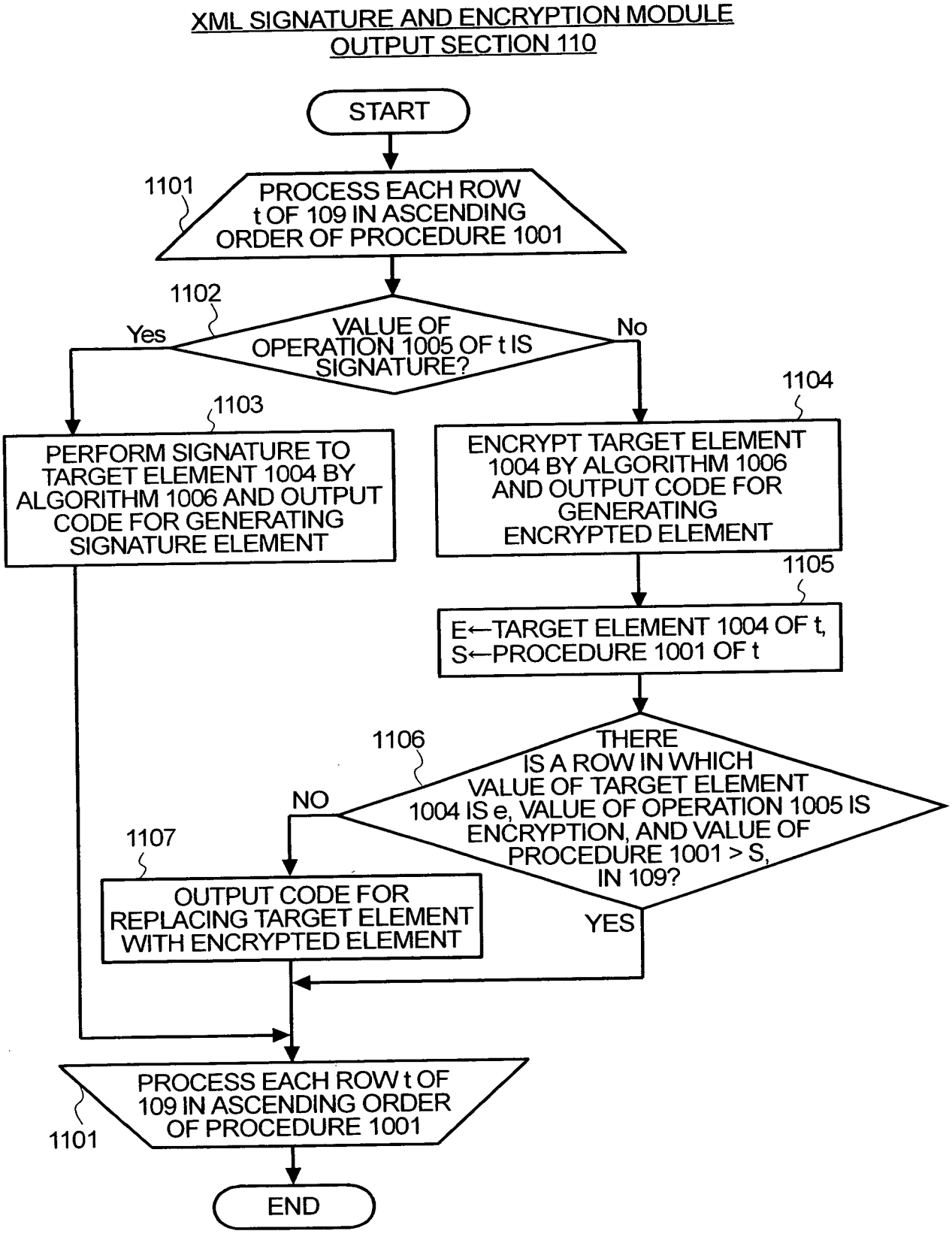

XML SIGNATURE AND ENCRYPTION MODULE OUTPUT SECTION 110
START
1101
PROCESS EACH ROW t OF 109 IN ASCENDING ORDER OF PROCEDURE 1001
1102
VALUE OF OPERATION 1005 OF t IS SIGNATURE?
Yes
No
1103
PERFORM SIGNATURE TO TARGET ELEMENT 1004 BY ALGORITHM 1006 AND OUTPUT CODE FOR GENERATING SIGNATURE ELEMENT
1104
ENCRYPT TARGET ELEMENT 1004 BY ALGORITHM 1006 AND OUTPUT CODE FOR GENERATING ENCRYPTED ELEMENT
1105
E←TARGET ELEMENT 1004 OF t, S←PROCEDURE 1001 OF t
1106
THERE IS A ROW IN WHICH VALUE OF TARGET ELEMENT 1004 IS e, VALUE OF OPERATION 1005 IS ENCRYPTION, AND VALUE OF PROCEDURE 1001 > S, IN 109?
NO
YES
1107
OUTPUT CODE FOR REPLACING TARGET ELEMENT WITH ENCRYPTED ELEMENT
PROCESS EACH ROW t OF 109 IN ASCENDING ORDER OF PROCEDURE 1001
1101
END

FIG.12

XML SIGNATURE AND ENCRYPTION MODULE111

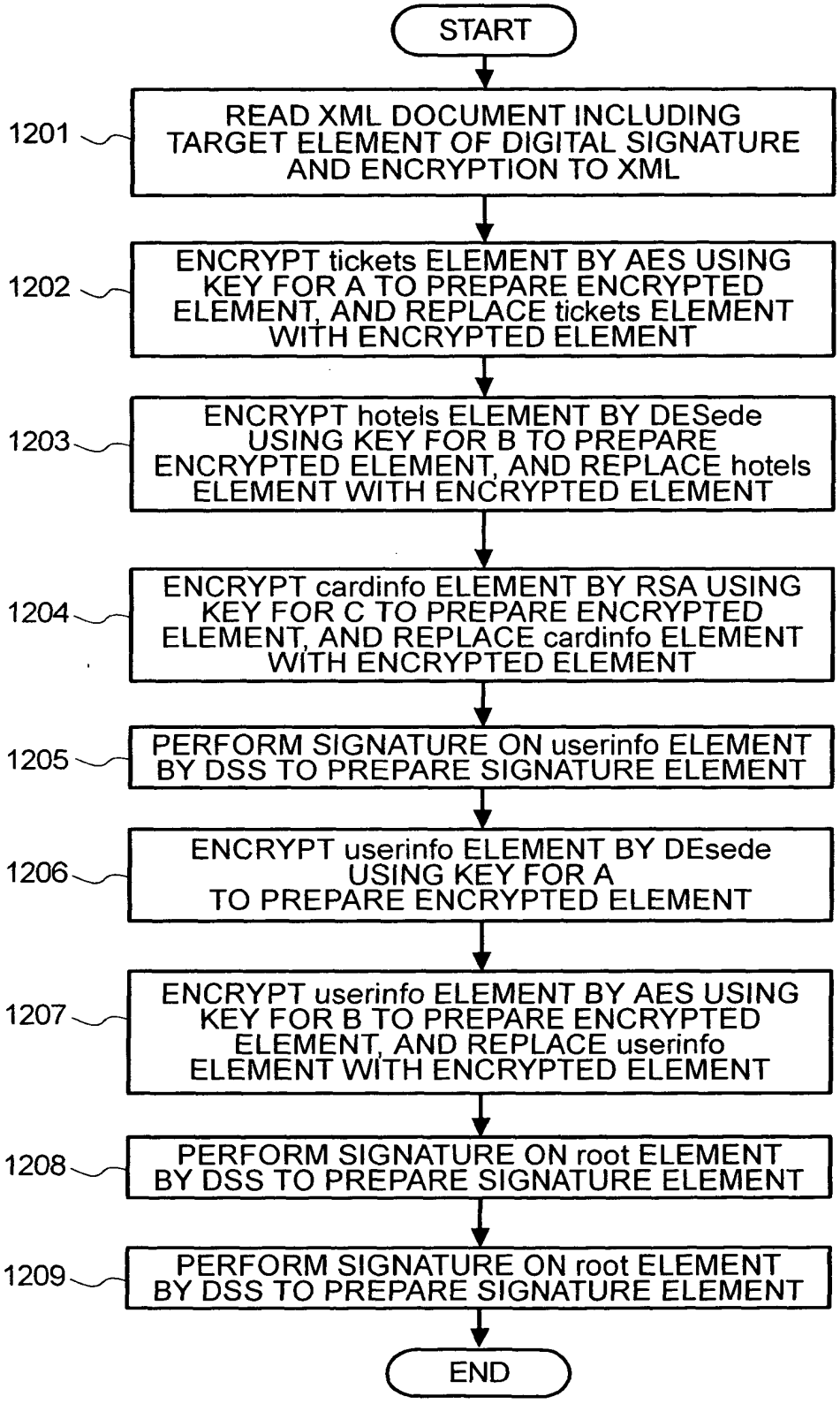


FIG.13

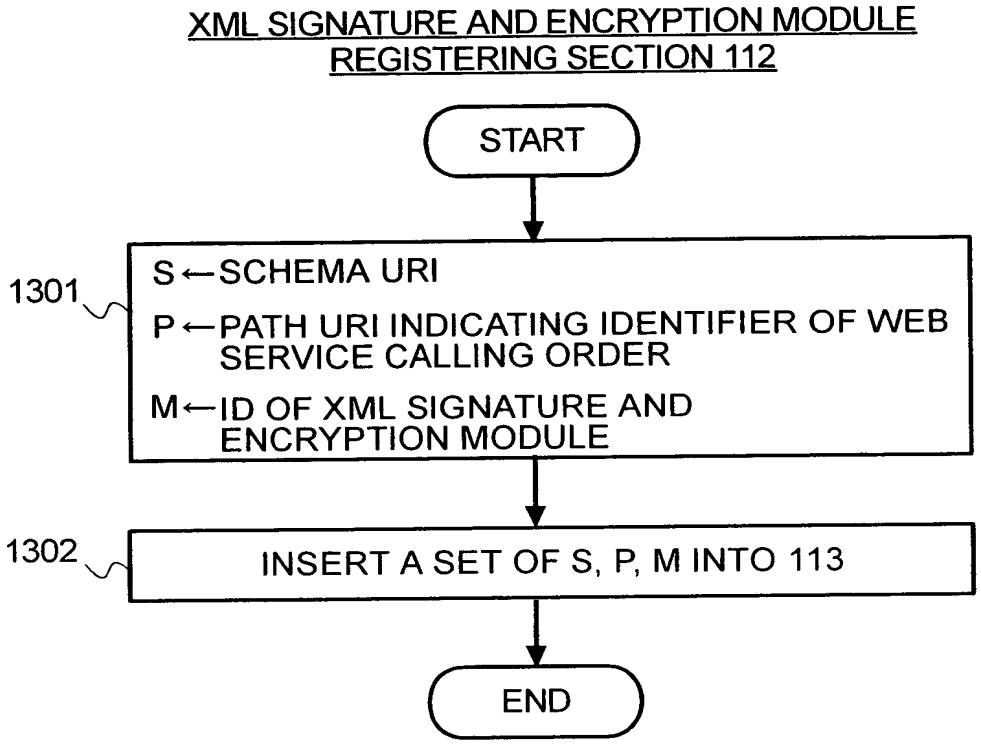


FIG.14

XML SIGNATURE AND ENCRYPTION MODULE CORRESPONDENCETABLE 113

	1401 SCHEMA URI	1402 PATH URI	1403 MODULE ID
1404	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/tp1	XMLSEC01
1405	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/tp2	XMLSEC02
1406	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/bp	XMLSEC03
1407	http://www.hitachi.co.jp/travel	http://www.hitachi.co.jp/pp	XMLSEC04

FIG.15

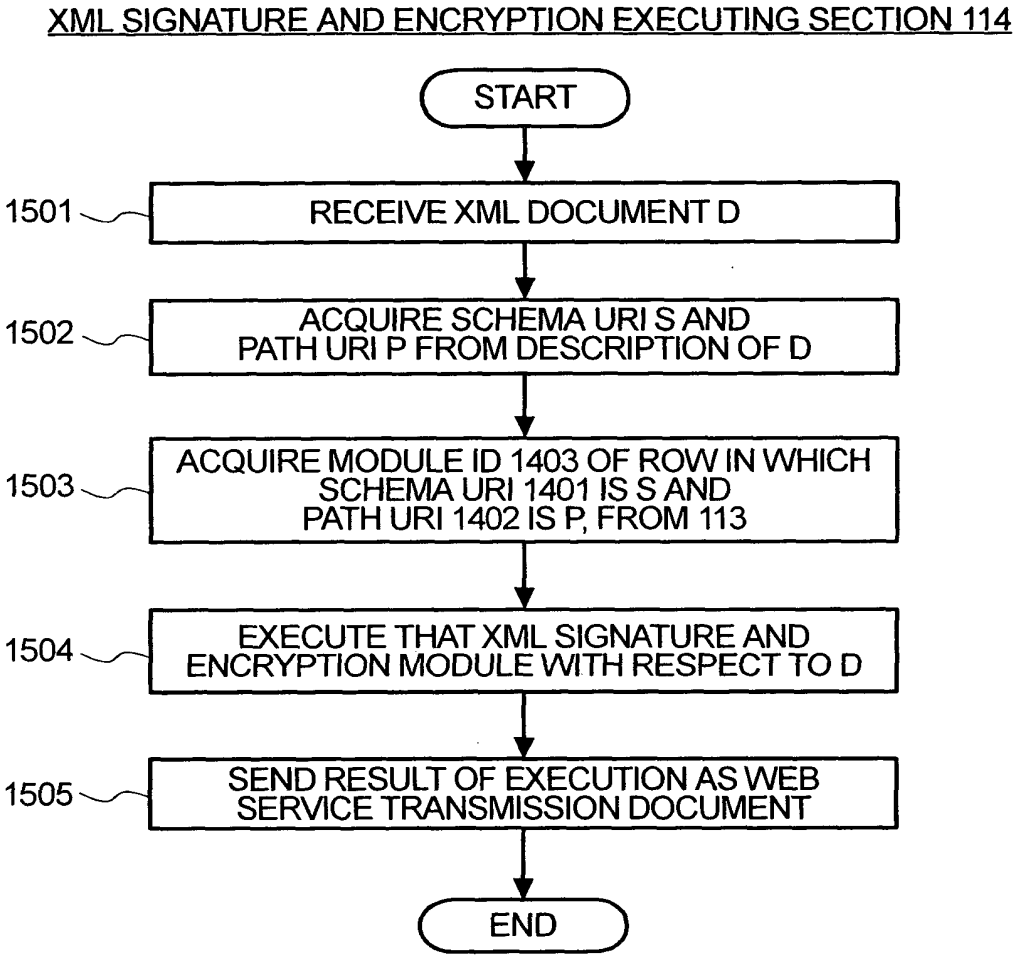

XML SIGNATURE AND ENCRYPTION EXECUTING SECTION 114
START
1501
RECEIVE XML DOCUMENT D
1502
ACQUIRE SCHEMA URI S AND PATH URI P FROM DESCRIPTION OF D
1503
ACQUIRE MODULE ID 1403 OF ROW IN WHICH SCHEMA URI 1401 IS S AND PATH URI 1402 IS P, FROM 113
1504
EXECUTE THAT XML SIGNATURE AND ENCRYPTION MODULE WITH RESPECT TO D
1505
SEND RESULT OF EXECUTION AS WEB SERVICE TRANSMISSION DOCUMENT
END

FIG.16

XML DOCUMENT 115

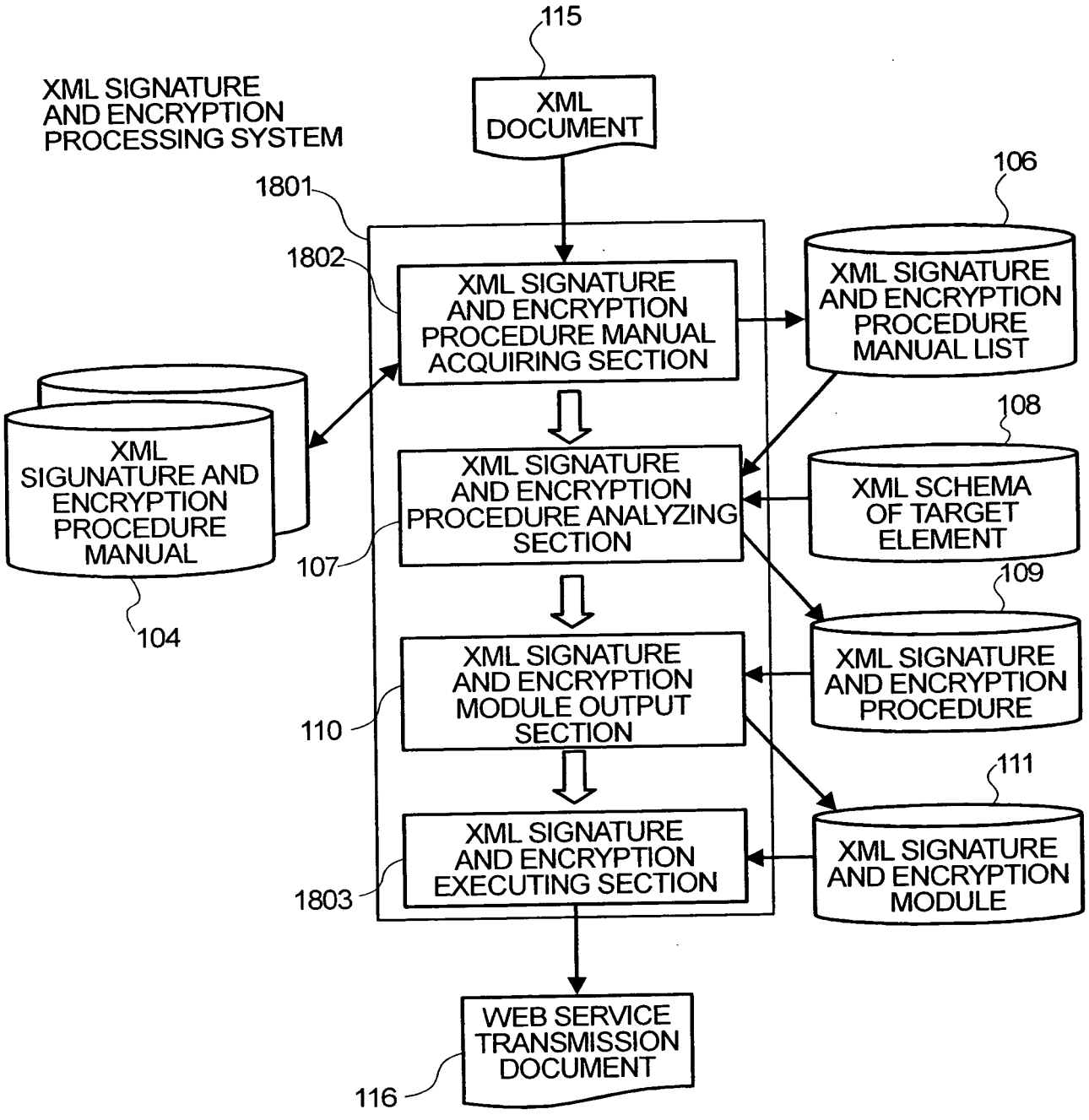
```
<?xml version="1.0" encording="Shift_JIS"?>
<message>
    <path xmlns="http://www.hitachi.co.jp/tp 1">
      <next URI="http://www.tickets.com/" />
      <next URI="http://www.hotels.com/" />
      <next URI="http://www.cards.com/" />
    </path>
    <root xmlns="http://www.hitachi.co.jp/travel">
      <tickets>
        <ticket from="TOKYO" to="OSAKA" date="02/04/01" time="09:00" />
        <ticket from="OSAKA" to="TOKYO" date="02/04/02" time="17:00" />
      </tickets>
      <hotels>
        <hotel name="HITACHI HOTEL" roomtype="S" date="02/04/01" />
      </hotels>
      <userinfo>
        <name>TARO HITACHI</name>
        <addr>CHIYODA-KU, TOKYO</addr>
        <cardinfo expiration="04/04"cardnumber="0123 4567 8901 2345" />
      </userinfo>
    </root>
</message>
```

FIG.17

WEB SERVICE TRANSMISSION DOCUMENT 116

```
<?xml version="1.0" encording="Shift_JIS"?>
<message>
  <path xmlns="http://www.hitachi.co.jp/tp 1">
      <next URI="http://www.tickets.com/" />
      <next URI="http://www.hotels.com/" />
      <next URI="http://www.cards.com/" />
  </path>
  <root xmlns="http://www.hitachi.co.jp/travel">
       <EncryptedData xmlns="http://.../xmlenc#" Recipient="TICKET ARRANGEMENT">
          <CipherData><CipherValue>AB...CD</CipherValue></CipherData>
       <EncryptedData >
       <EncryptedData xmlns="http://.../xmlenc#" Recipient="HOTEL RESERVATION">
          <CipherData><CipherValue>EF...GH</CipherValue></CipherData>
       </EncryptedData >
       <EncryptedData xmlns="http://.../xmlenc#" Recipient="TICKET ARRANGEMENT">
          <CipherData><CipherValue>HI...JK</CipherValue><\CipherData>
       </EncryptedData >
       <EncryptedData xmlns="http://.../xmlenc#" Recipient="HOTEL RESERVATION">
          <CipherData><CipherValue>LM...NO</CipherValue></CipherData>
       </EncryptedData >
  </root >
  <Signature xmlns="http://.../xmldsig#" Id="TICKET ARRANGEMENT">
      <Signature Value>ABC...DEF</SignatureValue>
  </Signature>
  <Signature xmlns="http://.../xmldsig#" Id="HOTEL RESERVATION">
      <SignatureValue>BCD...EFG</SignatureValue>
  </Signature>
  <Singnature xmlns="http://.../xmldsig#" ID="CARD SETTLEMENT">
      <SignatureValue>CDE...FGH</SignatureValue>
  </Signature>
</message>
```

FIG.18


XML SIGNATURE AND ENCRYPTION PROCESSING SYSTEM
115
XML DOCUMENT
1801
1802
XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL ACQUIRING SECTION
106
XML SIGNATURE AND ENCRYPTION PROCEDURE MANUAL LIST
XML SIGUNATURE AND ENCRYPTION PROCEDURE MANUAL
104
XML SIGNATURE AND ENCRYPTION PROCEDURE ANALYZING SECTION
107
108
XML SCHEMA OF TARGET ELEMENT
109
XML SIGNATURE AND ENCRYPTION PROCEDURE
XML SIGNATURE AND ENCRYPTION MODULE OUTPUT SECTION
110
111
XML SIGNATURE AND ENCRYPTION EXECUTING SECTION
1803
XML SIGNATURE AND ENCRYPTION MODULE
WEB SERVICE TRANSMISSION DOCUMENT
116